Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission concerning "Threats to European Commission interests in the areas of counter-intelligence and counter-terrorism"

Brussels, 26 January 2009 (Case 2008-0440)

1. Procedure

On 16 July 2008 the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Commission a notification for prior checking concerning "Threats to European Commission interests in the areas of counter-intelligence and counter-terrorism".

On 5 September 2008 the EDPS asked the controller for additional information. The replies were received on 12 September 2008. Further questions were put on 26 September 2008. The controller replied on 14 October 2008. A draft opinion was sent to the controller for comment on 6 November 2008. At the Commission's request, a meeting was organised on 4 December 2008 to clarify the facts. An amended opinion was submitted for comment on 19 December 2008. Comments were received on 23 January 2009 and on the same date the suspension of 6 November 2008 was lifted.

2. The facts

The ***purpose*** of the processing operation introduced by the ADMIN DS 02 unit is to protect the staff, buildings, information and activities of the European Commission as well as the interests of the Member States with regard to threats in the areas of counter-espionage and counter-terrorism.

The protection measures involve in particular (1) **conducting security investigations** and (2) **implementing security screening.**

1. Security investigations

Security investigations are conducted by members of the ADMIN DS 02 unit using relevant information made available by or requested from Member States as well as information collected within the institution. Decision 2001/844/EC establishes a comprehensive security system specific to the Commission under which there is provision to investigate or order an investigation into any leakage of EU classified information that, on prima facie evidence, has occurred in the Commission. In addition, the Security Office Charter of 8 September 1994 establishes that the Security Office should gather information to assess potential threats or risks to Commission departments and conduct investigations entrusted to it by the competent authority, or initiated on its own initiative when offenders are caught in flagrante delicto. To do so, the Decision specifies that the Office may hear staff members, or, in compliance with the rules on confidentiality, inspect any internal Commission documents in order to obtain information required for a security investigation.

(a) Conditions for initiating a security investigation

Security investigations may be initiated at the request of the Director-General of the DG concerned: such a request ensues if initial facts discovered suggest that a security offence may have been committed. The request is addressed to DG ADMIN or the Director of the Security Directorate. Following approval by the Director of Security, the DS 02 unit takes the necessary steps to validate the information received, then to determine the circumstances in which the facts occurred, and, where appropriate, to define the responsibilities of the staff members concerned.

A security investigation may also be initiated when, in the course of performing their duties, DS departments become aware of facts suggesting that a security offence has been committed and, after establishing the value of the information received, the Director of Security takes the initiative to request that DS 02 open an investigation intended to establish the facts and ascertain any responsibility. The DS 02 Head of Unit must be informed of any investigation being opened, as well as of its purpose and the background to it. These investigations are recorded in the DS 02 operational database (case number and file name as well as a brief description of the case).

(b) Conditions for implementing security investigations

Each investigation is assigned to an investigator in the Classified Information (CI) section of DS 02. All investigations are subject to the need-to-know rule both within and outside the section as well as outside the unit:

- Depending on the level of confidentiality and the need to know, the Head of Unit and the Head of Section determine the way in which the file must be handled (whether or not to inform other investigators in the section).

- The Head of Unit must systematically be notified in advance of any major action (interviewing a member of staff above Head of Unit level or interviewing a member of staff in respect of whom a question of responsibility arises).

- Any request to access a staff member's personal file or any action falling within the scope of the exemptions and restrictions provided for in Article 20 of Regulation No 45/2001 are subject to approval and signature by the Head of Unit and/or the Director of Security.

The Head of Section is systematically kept informed by the section investigators of meeting agendas and interviews, as well as of any action to be taken as part of investigations. For the purposes of validation, he informs the Head of Unit of the agenda for upcoming initiatives and of the direction the investigations are taking.

The Director is kept informed on a case-by-case basis, depending on the implications of each file, either in real time if deemed necessary by the DS 02 Head of Unit, or at least once a month during the bilateral monthly working plan meetings.

Since April 2008, cases and investigations underway have been presented at a monthly meeting in the Private Office of the Commissioner responsible for security issues, with the DS represented by the Director of Security and the DS 02 Head of Unit.

(c) The processing operation and the recipients of the final report

The final investigation report drawn up by the investigators is systematically submitted for the approval of the Head of Unit and the Director of the Security Directorate. In those cases where the investigation has been initiated at the request of a Commission Director-General, the final report is sent for signature by the Director-General for ADMIN, via the Director of the Security Directorate and the DS 02 Head of Unit.
In cases where the investigation was implemented at the initiative of the Director of the Security Directorate, the final report is sent by the Director-General of ADMIN to the Director-General of the DG concerned by the investigation.

Independently of the above, where responsibility *may have* disciplinary consequences or consequences which jeopardise the financial interests of the institution, the IDOC and/or OLAF are informed and the important elements of the file are forwarded to them. This always takes place via the hierarchical channel of the Head of Unit/Director of Security/Director-General of ADMIN. Where other parties of the Member States need to be informed either of the investigation underway or of the outcome, the DS 02 Head of Unit takes the decision to forward the information deemed necessary in agreement with the Director of the Security Directorate.

2/ Security screening

Threat management includes the security screening of any third-country national likely to be recruited by or win a contract at the Commission. At the request of the Directorates-General concerned (DGs have been instructed by ADMIN DS 02 to advise the Security Directorate prior to the recruitment or arrival of third-country nationals who may pose a threat with a view to their screening), ADMIN DS 02 contacts its counterparts (national security authorities) in the Member States to find out whether there are any reasons why the person should not be admitted to the institution. As part of the request, DS 02 will specify the general background to the file (future post, general characteristics, etc.). In this procedure, DS 02 works with all types of information, as opposed to the "yes/no" received from a national security authority in a clearance procedure. All screening is based on an advance assessment of the risks run by the institution. The assessment itself depends on the third country/countries possibly concerned, the current situation there, as well as the information which the DS receives from its partner departments in the Member States or other institutions. Assessment criteria are classified (they may for example be linked to the particular political situation, a conflict, or factors relating to the areas of competence concerned). The decision is taken on the basis of the risk that the individual may present for the institution (in the areas of data protection, terrorism or ordinary procedures).

A DG may also submit a screening request for a Member State national. Such a request would be at the initiative of the DG. ADMIN DS 02 decides whether or not to launch a screening procedure on the basis of the classified criteria and the advance assessment, both explained above.

The screening procedure arises from point 4.4(b) of Part I of Decision 2001/844/EC which states: "security measures shall (…) be designed to detect persons whose position might endanger the security of classified information and important installations housing classified information and provide for their exclusion or removal".

Based on the replies received, ADMIN DS 02 submits the appropriate recommendations to the requesting Directorates-General. The recommendations may be written or verbal or provide practical advice on additional security measures to be introduced. It may go as far as recommending that the person not be recruited. The recommendations will be communicated to the Local Security Officer (LSO) or the person responsible for recruitment.

Analysis of the information resulting from security investigations and screening also enable the ADMIN DS 02 unit to **produce assessments of threats** to the institution and analyses of specific situations.

3. Other information relating to security investigations and screening

Data processing procedures are ***manual*** or ***automated***. The mechanisms for liaising with Member State security departments, for example, and the resulting data, are automated, but a paper version of the data exchanged may also be produced and archived after they are circulated to authorised persons.

The ***data subjects*** are not the same in the two procedures. The data subjects of security investigations are Commission staff and any person who might pose a risk for the security of the staff members, information or assets of the institution, including visitors, journalists and even family members, but excluding the staff of other EU institutions. The data recipients of the screening procedure are people likely to be recruited by or win a contract at the Commission, particularly from third countries, who pose a threat to the institution.

All information relevant to the threat under consideration, in particular ***data*** supplied by the Member States, is processed. Such information may include data under Article 10 of Regulation (EC) No 45/2001 ("the Regulation"). DS 02 may request access to the Commission's databases. The data in this case are those administered by the Commission departments. The unit also possesses information from the intelligence and security services of the Member States, and, in this case, the data transferred are classified. Aspects relating to religious or political beliefs, convictions or suspicions may be included, provided that they are relevant to the risk to be assessed or the requirements of the investigation. With regard to access to data contained in electronic communications, DS 02 may request access to the content of e-mail exchanges when a security investigation has been opened, with the authorisation of the ADMIN Director-General and the prior agreement of the Data Protection Officer.

The data are ***stored*** as long as the threat to the institution remains in place and for as long as Member States may submit requests pertaining to these data. Classified information is processed in accordance with the specifications set out in Decision 2001/844, but on the basis that no decision affecting these documents may be taken without the consent of the originating department. With regard to screenings, the controller specifies that since the operation was introduced only recently, a time limit for storage has not yet been established. The controller plans to set a storage time limit of ten years. If necessary, ***erasure*** and ***blocking*** may be performed within 30 days of a justified request to that effect.

The data ***recipients*** vary according to the category of data. Investigation reports in the context of security investigations are sent to the departments concerned, depending on the investigation outcome (IDOC, OLAF, relevant Appointing Authority). For screening requests, the originating DGs receive only the recommendations relevant to the case. Other parties of the Member States may also be data recipients. Such parties could be the judicial authorities and the security and intelligence services of the Member States. In the event of a transfer to the judicial authorities (none has occurred to date), ADMIN DS 02 would draw up a reasoned decision proving the need for the transfer.

In the case of security investigations, the data subjects may exercise their ***rights*** via the controller. If one or more of the exemptions under Article 20 restrict the implementation of Articles 13 and 14, the data subjects may request that the processing operation be verified by the EDPS as provided for in Article 20(4) of the Regulation.

The data subjects are ***informed*** in a general way via the privacy statement published on the Security Directorate website and Europa portal. All staff members called to give a statement in the context of an administrative security investigation systematically receive the text of the privacy statement specific to the processing operation. The privacy statement sets out the remit of the ADMIN DS 02 unit (purpose of the processing operation), names the controller and the legal basis, refers to the recipients, the mandatory or optional nature of replying to the questions, the storage time limit, the source of the data and the data subject's rights of access and rectification. Persons undergoing screening will not normally be informed unless, for example, they appeal after they are turned down for recruitment and the DG justifies the refusal by stating the recommendations made by the Security Directorate. The Security Directorate would use the exemptions provided for in Article 20 of the Regulation if the threats to the institution still apply.

Some ***security measures*** have been taken (…).

3. Legal aspects

3.1. Prior checking

The prior checking relates to the processing of personal data ("any information relating to an identified or identifiable natural person", Article 2(a) of the Regulation) in the context of security investigations and screening conducted by the Commission's ADMIN DS 02 unit. The processing consists of operations to collect, consult, store, erase, etc. personal data.

The processing operation is carried out by a European institution in the exercise of activities which fall within the scope of Community law. The activities introduced by the ADMIN DS 02 unit are clearly intended to manage threats to the interests of the Commission in the areas of counter-intelligence and counter-terrorism. The legal basis, analysed in the following point, is partly the Commission Decision of 29 November 2001 (2001/844/EC, ECSC, Euratom). The Commission Decision of 31 January 2006 amending Decision 2001/844/EC adds a new recital after recital 7 of the Annex. It is worded as follows: "these provisions are without prejudice to Article 286 of the Treaty and to Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data."

Lastly, the processing of personal data is largely automated (Article 3(2) of the Regulation). The Regulation is therefore applicable in this case.

Article 27(1) of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

Article 27(2)(b) of the Regulation stipulates that operations intended to "*evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall be subject to prior checking by the EDPS. In this case, the data subject's conduct is analysed by the ADMIN DS 02 unit.

Furthermore, under Article 27(2)(a) of the Regulation, processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" are also subject to prior checking by the EDPS. In the case in point, the processing operation might concern this type of data.

Since prior checking is designed to address situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operation has already begun. This is not a serious problem here, though, as any recommendations made by the EDPS may still be implemented if necessary.

The DPO's notification was received on 16 July 2008. According to Article 27(4), this opinion must be delivered within two months following receipt of the notification. The procedure was suspended for 103 days + the month of August. The opinion will therefore be adopted no later than 28 January 2009.

3.2. Legal basis and lawfulness of the processing operation

Article 5(a) of the Regulation stipulates that personal data may be processed only if: "*processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*". The security investigations and checks conducted by the ADMIN DS 02 unit qualify as tasks carried out in the public interest (fight against threats to Commission interests in the areas of counter-intelligence, counter-terrorism, protection of classified EU information, etc.). The ADMIN DS 02 unit also performs these activities in the legitimate exercise of official authority and therefore complies with its legal obligation to examine matters within its remit.

Data processing in the context of security investigations and screening is based on various legislative instruments ranging from very general to very specific.

First of all, there is Commission Decision 2001/844 of 29 November 2001 relating to the Commission's security provisions. Point 5.2 sets out how security in the Commission is organised. With regard to security investigations, Point 24.2 on managing breaches of security and compromise of EU classified information sets out the role of the security officer and security authority in such cases. With regard to the screening procedure, point 4.4(b) on the aims of security measures states the following:

The security measures shall:

(b) be designed to detect persons whose position might endanger the security of classified information and important installations housing classified information and provide for their exclusion or removal.

The Commission Decision of 19 September 1994 on the duties of the Security Office (Decision C(94) 2129) describes the tasks of the Security Office in more detail, in particular:

in Article 3:

Ordinary tasks

The Security Office shall be responsible for the protection of persons, property and activities at the Commission.

Accordingly, its tasks shall include:
(a gathering information to assess potential threats or risks to Commission departments;
(b) studying proposals and implementing security measures intended to combat such threats or risks;
(c) informing Commission staff of obligations with respect to security;
(d) monitoring compliance with current security rules by Commission departments;

(e) maintaining order in Commission buildings within the framework of the applicable laws;
(f) conducting investigations entrusted to it by the competent authority, or initiated on its own initiative when offenders are caught in flagrante delicto, aimed at ensuring secure operating conditions in the Commission or at obtaining information relating to any illegal acts occurring in its departments for the purposes of a judicial inquiry or disciplinary action.

in Article 4:

Special powers

1. In order to protect the security of Commission departments, the President may, if the circumstances so dictate, require the Security Office to perform the following tasks, while ensuring the due respect for human rights and fundamental freedoms that is incumbent on the European Communities:
(a) check the identity of persons entering a Commission building, and if appropriate refuse them access;
(b) check the identity of persons within Commission buildings;
(c) inspect items carried by persons entering or leaving Commission buildings;
(d) confiscate as a precautionary measure any documents or objects relevant to an administrative investigation;
(e) hear staff members, or, in conformity with the rules on confidentiality, inspect any internal Commission documents in order to obtain information required for an administrative investigation.
2. Officials of the Security Office shall be authorized to carry a sidearm in accordance with the conditions laid down by the national laws in force, and in Commission buildings in accordance with the conditions laid down by the officers' superiors.
3. The Security Office may turn to a security firm to carry out, under the direction and the supervision of the Security Office, tasks relating to entry control.

Lastly, Article 6 of the Decision provides that:

The Security Office shall handle relations with:
(a) national security and intelligence services with a view to collecting the information required to assess potential threats and risks to the Commission;
(b) national authorities with respect to questions concerning the protection of Commission buildings, application of criminal laws and the immunity of officials from legal proceedings where matters of security are involved;
(c) the security services of other Community institutions with a view to developing a coordinated or common security policy.

The processing operation introduced by the Commission's ADMIN DS 02 unit complies with the security requirements clearly set out in the above legal instruments and therefore has a sound legal basis. This supports the lawfulness of the processing operation.

The EDPS wishes to point out, however, that the legal basis for the screening procedure is vague and rather general. Without questioning the need for such a procedure, the EDPS would like to see a more detailed legal basis covering a broader scope spanning all the possibilities for launching a screening procedure. The current legal basis restricts the procedure to "*the security of classified information and important installations housing classified information*". However, the threat to the institution or Member States could take any form and might concern non-classified information/areas. This aspect must be taken into account when establishing the new legal basis.

The "necessity" of the processing has to be analysed in specific terms. From this perspective, it has to be borne in mind that the processing of personal data conducted in the context of security investigations and screenings must be proportional to the general purpose of processing (protecting the interests of the institution and the Member States) and to the particular purpose of processing in the case in point (with regard, for instance, to the seriousness of the incident under investigation, the sort of data needed to clarify the facts, etc.). Proportionality must therefore be evaluated on a case-by-case basis. Subject to such case-by-case analysis, the lawfulness of the processing operation proposed is upheld.

3.3. Processing of special categories of data

Article 10(5) of the Regulation stipulates: *"[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards".* In the present case, processing of the data in question is authorised by the legal instruments mentioned in point 3.2 above.

Apart from that scenario, under Article 10(1) of the Regulation, the processing of special categories of data (that is "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life*") is prohibited. Article 10(2) of the Regulation provides for certain exceptions. The only exception likely to apply would be (d) (*processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims*(…)).

The type of data described in Article 10(1) will not be systematically processed but will undoubtedly feature in the context of investigations and screening procedures. If this happens, the general ban in Article 10(1) must be respected, or the need for an exception examined closely. In any event, the DS 02 unit staff responsible for the files must remember that these are exceptions and avoid including special categories of data, unless the circumstances provided for in Article 10(2)(d) arise in the case in question or it is necessary to apply Article 10(4) of the Regulation ("*Subject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor*").

3.4. Data quality

According to Article 4(1)(c) of Regulation 45/2001, personal data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*".

While certain standard types of data (name, category of person, etc.) will feature regularly in the screening procedure, the exact content of the files will, of course, vary from case to case. The same applies to security investigation files. Guarantees must therefore be established in order to ensure compliance with the principle of data quality. This could take the form of a general recommendation to the persons handling the files, reminding them of the rule and recommending that they ensure compliance with it.

With regard to the screening procedure, the EDPS welcomes the fact that DS 02 assesses the screening request from the DG before it is launched using the classified criteria at its disposal, thereby avoiding the collection of unnecessary data as part of a non-justified screening procedure. The EDPS would like it specified in the information notice that the screening procedure will only be triggered following evaluation (according to specific criteria) of the screening request by DS 02 in order to remove any ambiguity as to the arbitrary nature of the launch of such a procedure (see point 3.9).

According to Article 4(1)(d) of the Regulation, personal data must be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified*." The procedure in place must give sufficient cause to believe that the data are accurate and kept up to date. This principle is very much connected to the exercise of the right of access, rectification, blocking and erasure (see point 3.8 below).

Data must also be "*processed fairly and lawfully*" (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, considerable attention must be paid to this in the context of such a sensitive subject. It concerns the information given to the person who is the subject of an investigation (and other data subjects), and the speed with which this information is given, so that the right of defence can be respected (see point 3.9 below).

3.5. Storage of data

Personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes*" (Article 4(1)(e) of the Regulation).

The data concerning security investigations are stored as long as the threat to the institution remains in place and for as long as Member States may submit requests pertaining to these data. DS 02 has not therefore set a deadline for storage of these data. It is the EDPS's understanding that this analysis is carried out on a case-by-case basis for files which are, by nature, always individual. However, in order to ensure effective destruction of the data once the purpose for collection has been achieved, the EDPS recommends implementing a procedure preventing the data from being stored any longer than necessary.

With regard to data relating to the screening procedure, the EDPS considers the ADMIN DS 02 unit's proposal to store the data for ten years to be in compliance with Article 4(1)(e).

In addition, under Article 37(1), traffic data, i.e. the data necessary to establish calls, must be deleted or made anonymous at the end of the call. Exemptions to this principle are provided for in Article 20, in particular when the exemption is needed to safeguard "the protection of the data subject" or "the national security, public security or defence of the Member States".

Traffic data collected in an investigation are stored, like other data, as long as the threat to the institution remains in place and for ten years in the context of screenings. The data may be stored on the basis of the exemptions provided for in Article 20, if necessary.

3.6. Data transfer

3.6.1. Transfer of personal data within or between Community institutions or bodies

Article 7(1) of the Regulation stipulates: "*Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient*".

This means that reports and/or related documents (personal data) are transferred only if necessary for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard, taking into account, for instance, the nature of the data collected and further processed, and the competence of the recipient.

If data are transferred following a request from the recipient, both DS 02 and the recipient bear responsibility for the legitimacy of the transfer in accordance with Article 7(2). The controller is required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller must seek further information from the recipient.

In any case, in accordance with Article 7(3) of the Regulation, the recipient must be informed that personal data can be processed only for the purposes for which they were transmitted.

Furthermore, DS 02 must include a note in the file mentioning the transfer of data.

In the case under examination, the nature of transfers varies depending on the procedure. In the context of security investigations, data may be transferred to IDOC, OLAF and the relevant Appointing Authority, while in the context of the screening procedure data may be transferred (in the form of appropriate recommendations) to the LSO or the person responsible for recruitment in the relevant department.

In the case of screening, DS 02 evaluates upstream the need for the DG's screening request and restricts the information transmitted to what is strictly necessary (recommendations). It therefore complies with the requirements of Article 7(1) and (2).

3.6.2. Transfer of personal data to Member States

There are two scenarios for Member States:

(a) Member States in which the data protection legislation adopted for the implementation of Directive 95/46/EC covers the judiciary and the national security authorities;

(b) Member States in which the data protection legislation adopted for the implementation of Directive 95/46/EC does not cover the judiciary and the national security authorities.

In the case of the first scenario, Article 8 of the Regulation provides that: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or (…)".*

Thus, even if judicial and security authorities do not fall within the scope of Directive 95/46/EC, if the Member State, when transposing Directive 95/46/EC into national law, has extended its application to those public authorities, Article 8 of the Regulation must be taken into account.

Although under Article 8(a) of the Regulation it is up to the recipient to establish the interest and necessity of receiving the information, given the specific activities of DS 02 the EDPS understands this provision to mean that if the information is not sent at the request of the recipient, the sender should verify whether such a need exists. Accordingly, if DS 02 sends personal information to competent national authorities on its own initiative, it must establish that the data are necessary for the performance of a task carried out in the public interest. DS 02 must conduct an evaluation each time it transfers personal data and establish a reasoned decision stating the need for the transfer. The EDPS welcomes the fact that DS 02 intends to draft such a decision in the event of a transfer to the judicial authorities in the context of security investigations. For the record, no such transfer has yet occurred. As for the screening procedure, DS 02 complies with this requirement as it conducts an upstream evaluation of the need to make a request to the national security authorities. It should be noted that in this procedure the request for information from the national security authority (accompanied by the name of the person, vacancy to be filled, etc.) is the only transfer that occurs.

For Member States that have not extended their implementation of Directive 95/46/EC to judicial, security or other relevant authorities, consideration must be given to Article 9 of the Regulation. In those countries, Council of Europe Convention 108, which in this case may be considered as providing an adequate level of protection, applies in any case applicable to judicial authorities.

3.6.3. Transfer to third country authorities and/or international organisations

Where personal data are transferred to third country authorities and/or international organisations, Article 9 of Regulation 45/2001 applies. The EDPS wishes to stress that such transfers are exceptional and that this point is being added to the analysis only in order to cover all eventualities of the processing operation. DS 02 has not to date had any instances of such transfers.

Article 9(1) of the Regulation provides that "*personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out*". Transfers to States not providing an adequate level of protection are therefore, in principle, not possible.

However, Article 9(6) stipulates that derogations are possible, in particular if "*the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims*" (Article 9(6)(d)). Since the provision is an exception, it should be interpreted strictly. The derogation may not, therefore, be used systematically. It may be used only occasionally, where the transfer is specifically needed in relation to the purpose of the processing operation. Use of Article 9(6) may not, under any circumstances, create a situation in which the fundamental rights of the data subject are violated.

Another possibility for DS 02 is to ask the EDPS to authorise the transfer, as provided for in Article 9(7), which stipulates that a transfer may be authorised by the EDPS "*where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses*".

Under Article 9(8), DS 02 must inform the EDPS of categories of cases where it has applied Article 9(6) and (7). For that purpose, the EDPS recommends introducing a register of occasional transfers carried out by virtue of the derogation under Article 9(6) and the authorisation granted under Article 9(7). The register could contain the following information: purposes of the transfer, data subjects, categories of data, information given to the data subjects (if applicable), rights of access (direct or indirect), legal basis and legality of the transfer, data recipients, indication of the length of time the data will be stored by the data recipient, etc. The register should always be available to the EDPS.

The EDPS is aware that point 26 of Part II of Decision 2001/844/EC sets out the principles governing the release of EU classified information to third States or international organisations. Point 26.1.1. stipulates, inter alia, that: "*the acceptance of EU classified information by third States or international organisations will imply an assurance that the information will be used for no purposes other than those motivating the release or exchange of information, and that they will provide the protection required by the Commission*". The EDPS highlights this point as it welcomes the fact that such transfers are subject to the strict security conditions established by Decision 2001/844/EC. However, it would point out that the transfers must also, as explained above, meet the data protection conditions provided for in Regulation 45/2001.

3.7. Confidentiality of communications

Under Article 36 of Regulation 45/2001, "Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law".

Electronic communications which are tapped in the course of security investigations come under Article 36 of Regulation 45/2001 and any restriction of the confidentiality principle must be "in accordance with the general principles of Community law". The concept of "general principles of Community law" refers to the fundamental human rights enshrined in particular in the European Convention on Human Rights.

In practice, this means that any restriction on the principle of confidentiality of communications must be consistent with the fundamental human rights enshrined in the European Convention on Human Rights. Such restriction may take place only if it is "in accordance with the law" and "is necessary in a democratic society" in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The fact that the agreement of the Commission's Data Protection Officer is required when competent departments access data concerning the data subject's workstation(s) constitutes an additional safeguard of compliance with Article 36 of the Regulation.

The EDPS considers that the requirement to ensure with the confidentiality of communications may be waived only in exceptional circumstances, in the course of a security investigation in which no less invasive means can be used. In any event, setting aside the requirement of confidentiality of communications cannot be the normal procedure, and must always be restricted to data which are strictly necessary.

3.8. Right of access and rectification

(a) Security investigations

Under Article 13 of the Regulation, the data subject has the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing processing and of any available information as to their source.

The right of access is the right of the data subject to be informed of any information relating to him/her that is processed by the data controller. On principle, this right must be interpreted in tandem with the notion of personal data. A broad view of personal data is used in the Regulation, and the Article 29 Working Party has also interpreted it broadly[1]. Compliance with the rights of access and rectification is directly connected to the data quality principle and, in the context of investigations, it overlaps to a great extent with the right of defence.

Furthermore, the right of access also applies when a data subject requests access to the files of other persons, if they contain information relating to him/her. This happens when informants or witnesses request access to the data relating to them in investigations conducted into other persons.

The information can be obtained directly by the data subject ("direct access") or, under certain circumstances, by a public authority ("indirect access", normally exercised by a Data Protection Authority, in the present context by the EDPS).

As stated in point 2 of this opinion, the data subject may approach the controller to exercise his/her rights. The EDPS understands that the two rights may be restricted in certain circumstances under Article 20 of the Regulation (see below). These restrictions must be "necessary" and must not under any circumstances become the general rule. The "necessity test" must be applied on a case-by-case basis and, like the right of information, the rights of access and rectification must be guaranteed as long as this would not be harmful to the investigation (see below point 3.9).

Article 20 of the Regulation therefore provides for certain restrictions on this right, notably where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences*; *(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others*". Moreover, in certain cases it may be necessary not to allow the data subject direct access, so as not to compromise the investigation, even where there is no criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001, but a "pre-disciplinary" or "pre-criminal" investigation. The interests of the authority which will follow the investigation (IDOC, OLAF, national authorities) may also be taken into account in this respect.

[1] See Opinion 4/2007 of 20 June 2007 on the concept of personal data adopted by the Article 29 Working Party (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf)

In any case, Article 20(3) must be considered and complied with by DS 02: *"If a restriction provided by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor."* Concerning the right to information, this provision has to be read in conjunction with Articles 11, 12 and 20 of the Regulation (see below point 3.9).

Account should also be taken of Article 20(4): *"If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made."* The indirect right of access must then be guaranteed. This provision will come into operation, for instance, in cases where the data subject has been informed of the existence of the processing, or has knowledge of it, but his or her right of access is restricted under Article 20.

Article 20(5) states that "*provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect*." It may be necessary for DS 02 to defer such provision of information under this provision, in order to safeguard the investigation. The need for deferral must be decided on a case-by-case basis.

As already mentioned, the right of access involves the right of the data subject to be informed of the data referring to him/her. However, as noted above, this right may be restricted to safeguard "*the protection of the (...) rights and freedoms of others*". This analysis must take this factor into account with regard to access by the data subject to the identity of whistleblowers. The Article 29 Working Party has made the following statement: *"[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblowers from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed*." The same approach has to be applied to informants[1].

Article 14 of the Regulation gives the data subject a right to rectify inaccurate or incomplete data. Given the sensitivity of most security investigations conducted by DS 02, this right is of key importance in guaranteeing the quality of the data used, which, in this case, is connected to the right of defence. The right of rectification also means that third party recipients are notified of rectifications to inaccurate or incomplete data, in accordance with Article 17. Any restriction under Article 20 of the Regulation must be applied in the light of what has been said in the preceding paragraphs regarding the right of access.

[1] Witnesses, on the contrary, do not require the confidentiality of their identity.

(b) Screening procedure

Articles 13 and 14 of Regulation 45/2001 also apply to the screening procedure. Given the sensitivity of the data processed in this context, the exemptions provided for in Article 20 will probably apply. The right of access is, however, a fundamental principle that must be guaranteed for the data subject. Each request for access must therefore be examined on a case-by-case basis and must not be systematically refused. There is always the possibility that the supposed threat may turn out to be unjustified and the direct right of access may therefore be granted. This fundamental principle must be expressed in the general information given to the data subjects even if the exemptions provided for in Article 20 are applied in practice (see point 3.9).

3.9. Information to be given to the data subject

(a) Security investigations

The Regulation states that the data subject must be informed where his or her personal data are being collected and lists a number of obligatory points to be included in the information, in order to ensure that the data are processed fairly. In the case at hand, the data could be collected directly from the data subject or indirectly, for instance through informants.

The provisions of Article 11 of the Regulation (*Information to be supplied where the data have been obtained from the data subject*) and Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) are thus both applicable to investigations. This means that the relevant information must be supplied either at the time it is obtained (Article 11), or when the data are first recorded or disclosed to a third party (Article 12), unless the data subject has already been given the information.

The type of information given to data subjects is described in detail in point 2.6. The document is entitled: privacy statement - data protection, and published on the Commission intranet and the external Europa portal. The statement is also given to anyone called to make a statement in a security investigation. Information is therefore given at two levels for security investigations: general information for all persons potentially concerned by the processing operation and specific information where a person is directly involved in a security investigation, and the EDPS welcomes this arrangement.

With regard to the point which the information must be given, when intelligence activities are conducted as part of an investigation, the information has to be given when appropriate, thus when it will not compromise the investigation. The point at which the information is provided may differ from the point when the data are first recorded or disclosed, in the light of Article 20 of the Regulation (see below).

Where DS 02 takes no written statement and has had no contact with the person before disclosing the data to a third party (OLAF, IDOC, national authorities), DS 02 must, under Article 12 of the Regulation, inform the data subject at the time of recording the personal data or no later than the time when the data are first disclosed to third parties. This recommendation obviously does not concern situations where contact with the data subject is impossible for practical reasons (where the person has disappeared or is on the run, etc.).

Article 20 of the Regulation provides for certain restrictions on the right of information while complying with the recommendations made by the EDPS in point 3.8. above.

Furthermore, Article 20(5) of the Regulation will have to be applied in specific circumstances: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect"*. (Paragraph 3 provides for the right of the data subject to be informed of the reasons why a restriction has been imposed as well as his right to have recourse to the EDPS; paragraph 4 provides for the indirect right of access via the EDPS and for the results of such access to be provided to the data subject).

As explained for the rights of access and rectification, the EDPS realises that the information given to the data subject may be restricted under Article 20 of the Regulation in certain circumstances (see above). Such restrictions must, however, be "necessary". The "necessity test" has to be conducted on a case-by-case basis, as is the case for the rights of access and rectification. The provision of information to the data subject must be guaranteed where it does not risk jeopardising the investigation. Restrictions on the right of information of the data subject must not under any circumstances become the general rule.

(b) Screening procedure

Only Article 12 applies to the screening procedure. Data are never collected from the data subject.

Although the content of the information supplied in the privacy statement matches the information that must be supplied under Articles 11 and 12, the EDPS has reached the conclusion that the information concerning the screening procedure is too vague to ensure that data subjects receive fair treatment (the data subjects are not, for example, only contractual staff). Data subjects should receive the privacy statement individually or at least be sent a link to it (a link to the privacy statement in the recruitment notice, for example, could be a general but direct means of information). Since the procedure is in principle totally unknown to the data subjects (as opposed to a classic recruitment procedure) and they will not naturally seek information on it, such information should be supplied pro-actively. This general information procedure is all the more important as there is no individual information procedure for screening.

The EDPS wishes to emphasise that the restrictions provided for in Article 20 must not be applied systematically but rather should be handled on a case-by-case basis. The last sentence of point 1.2 of the statement should therefore be amended accordingly.

The section on the time limit for data storage must be amended for the screening procedure in line with the time limit adopted by DS 02. The section on the legal basis must be amended in line with the new texts adopted.

3.10. Security measures

Some security measures have been taken. The conditions for data protection and physical access are those required by the Commission Decision of 29 November 2001 adopting the Commission's security rules (2001/844/EC). Generally speaking, physical and computer access is restricted to staff with the need to know and with the appropriate security clearance.

The EDPS considers that the full set of security measures taken can be regarded as adequate within the meaning of Article 22 of the Regulation.

Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation (EC) No 45/2001 provided that the considerations in this opinion are fully taken into account. In particular, DG ADMIN DS must:

- evaluate the proportionality of the processing activities on a case-by-case basis;
- establish a more detailed legal basis covering a broader scope spanning all the possibilities for launching a security screening procedure;
- introduce a procedure ensuring that data are stored no longer than necessary under Article 4(1)(e);
- introduce, in accordance with Article 7(1) of the Regulation, notice to the recipient informing him/her that personal data may be processed only for the purposes for which they were transmitted;
- in the context of investigations, check the competence of the recipient and make a provisional assessment of the need to transfer data when the recipient submits a transfer request in accordance with Article 7(2);
- transfer reports and/or related documents (personal data) only if necessary for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard;
- include a note in the investigation file mentioning the transfer of data;
- introduce a register of occasional transfers conducted by virtue of the derogation in Article 9(6) and (7) and notify the EDPS of any such transfers;
- revise the screening section of the privacy statement;
- pro-actively supply data subjects of screening with the privacy statement in accordance with Article 12;
- insert the time limit for data storage under the screening procedure into the privacy statement;
- in the context of investigations, inform the data subject at the time of recording the personal data or no later than the time when the data are first disclosed to third parties;

- mention in the file when any restriction based on Article 20 of the Regulation is imposed;
- inform the data subject in compliance with Article 20(3) and (4) of the Regulation where appropriate.

Done at Brussels, 26 January 2009.

(**signed**)

Peter HUSTINX
European Data Protection Supervisor (EDPS)